

REMARKS

Amendments to Claims

The Examiner rejected the drawings for not having the words “Replacement Sheets” in the upper margins. Such sheets are enclosed herewith with the appropriate “Replacement Sheets” in the upper margins.

The Examiner rejected, under 35 U.S.C. 112, second paragraph, claims 16, 18 and 25 as lacking an antecedent for “the set of encrypted single values.” The antecedent is supplied herein. Claims 20 and 26 were rejected under the same statute citing “a number” as leading to indefiniteness. That indefiniteness is corrected herein by using “quorum” that is found in the original application. No new matter is added.

Claims 16, 18, 25 and 31 are amended to more clearly point out that the generating, sending, and creating steps are done before the software product is encrypted to more clearly point out that these limitations are necessarily first performed to create the encryption key.

Although the Applicant will show below that the present Claim 28 is patentable over Larose and the Larose + LeBourgeois combination, Claim 28 is nevertheless amended to point out that the generating and sending of the first set of parameters are both done in response to the executing, the limitation of *storing* was added to point out that the *generating and sending* of the second set of parameters is performed in response to a user instructing a software application to download the software product. No new matter is added, see page 9 lines 28 - page 10 line 3, and page 15 line 24 of the application.

Claims 17 19, 22, 24, 27, 29, and 32 are amended to more clearly define the claim language. No new matter is added.

Finally, the Applicant adds three new independent apparatus claims: 37, 38, and 39, that correspond to method claims 23, 28, and 31, respectively.

Matyas does not disclose, or suggest, Claim 16

The Examiner rejected, under 35 U.S.C. 103(a), claim 16 as being unpatentable citing U.S. pat. No. 4,757,534 to Matyas et al. (Matyas) in view of U.S. pat. No. 6,212,635 to Reardon (Reardon) and U.S. pat. No. 6,049,612 to Fielder et al. (Fielder).

Respectfully, the Applicant believes there is some confusion with the Matyas patent. Matyas' patent discloses a software vendor who encrypts a software program with a unique encryption key "KF" and stores the encrypted program to a diskette that is then distributed for purchasing by users. In Matyas—before the software program has been encrypted—there is no *generating* of a first set of parameters from a user's computer and no *sending* of such a set of parameters---- in direct contrast with the first two limitations of Claim 16 that must occur before the creation of the encryption key:

"generating a first set of parameters from the computer before the software product is encrypted at the server,

sending the first set of parameters to the server computer before the software product is encrypted at the server,"

Both of these elements must be performed before the encryption of the software product since these steps are required to create the encryption key. Claim 16 has been amended to make this clearer.

The Examiner incorrectly cites, on page 4 paragraph 13a of the Office Action, that Matyas' "*Computer #, Disk#, and Prog#*" in his Fig. 3 discloses the above two elements. This is incorrect since the "*Computer#, Disk#, Prog#*" is information sent to the software vendor in Matyas *after the creation* of the encryption key KF used to encrypt the software program. Moreover, this is information the user gathers from the diskette

containing the encrypted software program and gives to the software vendor not to create the encryption key¹ but rather to obtain a password for the user:

“A user, who purchases a diskette containing an encrypted program, must first obtain a authorization number and password from the software vendor.”
(Matyas 5: 8-9, emphasis added).

“The procedure [for obtaining the password] is illustrated in FIG. 3. After purchasing a diskette, the user places a telephone call to the software vendor...S/he provides the software vendor with the program number...diskette number, and the computer number.” [i.e. the “‘Computer #, Disk #, and Prog #’” cited by the Examiner.] (Matyas 5: 62 6:2, emphasis added).

Therefore, Matyas Fig. 3, the “‘Computer #, Disk #, and Prog #’”, and related passages (e.g.. see Matyas 5:62- 6: 1-68) is a disclosure of the steps of his invention after the creation of his encryption key KF and indeed after using KF to encrypt the software program. In fact this is information sent to the vendor after the user obtains the encrypted software program². Clearly then the *generating* and *sending* of the first set of parameters of Claim 16 are both not found in Matyas.

In fact there are no stated problems, issues, or advantages in Matyas in short there is no motivation within Matyas that would suggest the *generating* and *sending* of the first set of parameters before creation of the encryption key KF used to encrypt the software product. *Before* software program is encrypted with KF—and indeed before the creation of KF itself—*there is no connection whatsoever* between the user and the software vendor. Indeed, a first connection between the user and vendor is first established in Matyas after the encryption key KF has already been created; and in fact, after the user has already obtained the diskette containing the encrypted software program (see above). There are no stated problems, issues, or advantages in Matyas that would suggest that the user

¹ The encryption key KF has *already* been created *and* used to encrypt the software program, which indeed has already been sent to the user.

² Therefore the cited information gathered by the user cannot be used in Matyas to create the encryption key KF used to encrypt his software program

make a connection to the software vendor before creation of the encryption key to then perform the *generating and the sending* elements necessary to create KF from such information. Matyas' 1987 time-frame only underscores this point. The only way to motivate one skilled in the art to modify Matyas to first perform these two elements of Claim 16, is to look at the present invention for motivation—which is impermissible.

Therefore, there exists sufficient reason to remove Matyas as a primary reference and allow Claim 16 as amended.

Although superfluous, the Applicant also wishes to briefly state that other elements of Claim 16 are dependent upon the elements discussed above and missing in Matyas; and therefore, these other elements are not and cannot be disclosed or suggested by Matyas; such as, 'encrypting the single value to form a set of encrypted values,' 'sending set of encrypted single values,' and 'decrypting the software product using the single value' since Matyas does not and cannot create such a single value per Claim 16 (see below). And, although again superfluous, the Applicant also wishes to briefly state below why the combination of references cited by the Examiner also cannot disclose or suggest Claim 16.

The Matyas, Reardon combination by the Examiner is inoperative and inconsistent with each reference. The Examiner does agree that Matyas does *not* disclose the element:

"creating, at the server computer, a single value from the first set of parameters before the software product is encrypted at the server,

of Claim 16, but states that Matyas *in light of Reardon* does. However, since Matyas does not generate any parameters from the user's computer and does not send such a set before creating his encryption key KF --used to encrypt his software program --adding Reardon's "seed" is therefore inoperative. It is inoperative and inconsistent to use Reardon's "seed" as the single value created from a set of parameters as in Claim 16,

when such a set of generated parameters in Matyas does not exist as already discussed³.

Additionally, therefore, this combination of references also does not, and cannot, disclose the next element Claim 16 of: “*encrypting, at the server computer, the software product by using the single value as the encryption key...*”⁴

Therefore by definition, adding *Fielder* cannot help, and in any event yields a combination of references that are inconsistent with each other; and therefore, cannot disclose the *creating and encrypting* elements of Claim 16. The Examiner states that Reardon discloses using the single value—not as a symmetric key as required in Claim 16—but as an asymmetric key. The Examiner then points to a combination of Matyas in view of Reardon *further in view of Fielder* with the additional argument that that since symmetric keys are more efficient than asymmetric keys, that then one skilled in the art would use this 3-fold combination of references with symmetric keys.

However, efficiency is not a motivation of Reardon’s, and the Examiner’s use of efficiency is not defined. Since protection is the fundamental motivation in *Fielder* (see his ABSTRACT), and PPK’s are, in certain contexts like *Fielder*’s, better than symmetric keys for protection, there is no motivation for Reardon to consider a symmetric key. If using a symmetric key were indeed more “efficient” than using an asymmetric key, and certainly Reardon knew about the much older symmetric key encryption, why would Reardon disclose only using an asymmetric key? In fact, under certain conditions and

³ The Examiner had cited Matyas in view of Reardon--- Column 10: 54-55, to disclose creating the single value from a set of parameters per Claim 16. However, here Reardon discloses creating a unique seed to generate a private/public key pair that would be unique to a security gateway and the Examiner also agrees that this key pair (e.g. PPK) is not the symmetric key as created in Claim 16.

⁴ The Examiner stated at page 4 paragraph 13b of the last Office Action that Matyas 6:59-62 discloses the *creating* a single value (though not from the set of parameters) and *encrypting* the software product with it. Respectfully, the Applicant believes this is just not the case. The cited passage of Matyas is not a discussion of creating his encryption key KF nor is it a discussion of using it to encrypt his software program; rather, it is a discussion of how a password is generated and given to the user *after* Matyas’ software program has already been encrypted with KF and sent to the user. The procedure of a user obtaining a password is shown in Matyas FIG 3 and described throughout Matyas Column 5:62 – Column 7:6.

contexts (e.g. Reardon's) it is often desirable to use an asymmetric key over a symmetric key.

In summary, not only is the Matyas/Reardon combination inoperative and inconsistent, adding Fielder's symmetric keys is, in any event, *inconsistent to Reardon's teaching*, and therefore this three-fold combination of references is inconsistent with each other. It is clear that these references cannot be combined consistently with each other to anticipate or suggest claim 16 as amended.

Matyas does not disclose, or suggest, Claim 17 dependant on Claim 16

The Examiner stated at page 6 paragraph 16 of the Office Action: "*As per Claim 17, Matyas covers a process as outlined above in Claim 16 rejection under 35 U.S.C. 103(a). In addition, the software product comprises data files or streaming data or both. See Matyas, claim 1. The aforementioned covers claim 17.*"

First, please note that the present application, and not Matyas, states "*software product comprise data files or streaming data or both.*" It appears that the Examiner has confused this statement of the present invention with Matyas—which in fact has no such language or suggestions. Second, Matyas' claim 1 simply does not state or suggest "*the software product comprises data files or streaming data or both.*"

Matyas does not disclose, or suggest, Claim 18 and 25

The last Office Action rejects Claims 18 and Claim 25 under 35 U.S.C. 103(a) for the same reasons used to reject Claim 16. Therefore, in light of the discussion above, Claims 18 and 25 should now also be allowed.

In any event, please also notice that unlike Claim 16 (and similar Claims 21, 23 and 31), Claim 18 and Claim 25 do not encrypt the software product. None of the cited references disclose or suggest the process of Claims 18 and 25 to thwart unwanted usage of the software product by sending the program unencrypted while sending an encrypted authorization artifact. Such a process has advantages, e.g., sometimes it's advantageous to protect the software product without encrypting it.

Matyas does not disclose or suggest Claims 21, 23, and 31

The Examiner had rejected Claims 21, 23, and 31 (at page 6 paragraphs 18, 19, and page 7 paragraph 21 respectively) for reasons cited for the rejection of Claim 16. Therefore, in light of the above, Claims 21, 23, and 31 should now also be allowed.

Overview of the Larose invention

Larose generates a first set of parameters and sends this set to a sever—and without any *generating* or *comparing*—his software product is then downloaded to the user's computer. Later, a second set of parameters is generated and a comparison is performed at the user's computer; and if the two sets match, the already downloaded software product is then *installed*. In Larose: no download authentication is performed, his comparing is not performed at a (secure) sever but instead at the (unsecured) user's computer; and, this comparison is only performed for the purpose of installing the already present software product. In short, unlike the present invention, the Larose invention is unable to authenticate the *download* of a software product to a computer.

Larose does not disclose, or suggest, Claim 28

The Examiner stated that Larose 12:33 – 13: 31 discloses *generating* the second set, *comparing* the first and second sets, and if they match, *installing* the software product--where apparently the Examiner equates Larose's *installing* to Claim 28's *downloading*.

Respectfully, the Applicant would like to point out that “*installing*” is not the same as “*downloading*” found in Claim 28, and indeed Larose uses these two terms in two distinct and separate actions, where the later occurs before the former. Larose's *comparison* does not result in any downloading because the software product (i.e. his *aggregate distribution file 170*) has already been downloaded when he generates the second set and performs the comparison (see Larose Column 11, Steps 8-9)---done for the sole purpose of allowing its installation. The Examiner agrees that Larose does not disclose the *generating* and *sending* of the second set nor the *comparing* at a server—all required for the secure authentication of downloading the software product, and elements of Claim 28.

Larose in light of LeBourgeois is inoperative and inconsistent with each reference, and does not disclose, or suggest, Claim 28

The Examiner states on page 8 paragraph 24 of the last Office Action that: “*LeBourgeois teaches submitting a second set of parameters to a server from a user prior to executing a transaction and comparing the second set...with the first set... at the server.*”

First, if one skilled in the art used the Larose invention, and then sent the second set of parameters to the server as taught by LeBourgeois, no comparison could be made by Larose because the Larose mechanism that performs any such comparison of first and second sets resides at the installation computer and not at the server. Therefore, this Larose + LeBourgeois combination contemplated by the Examiner cannot perform or suggest the required comparison at the server in accordance with Claim 28.

Second, the Examiner equates the “*transaction*” of LeBourgeois to the “*downloading*” of the present invention. Nowhere in LeBourgeois is the word “*transaction*” equated to or used in a way that would suggest “*downloading*.”

Third, Larose *first* downloads *and then* generates the second set of parameters to authenticate. However, LeBourgeois teaches generating the second set “*prior to executing a transaction*.” LeBourgeois cannot be true or consistent to his invention if his “*transaction*” occurs before his authentication of the user. Therefore, the LeBourgeois teaching cannot be combined consistent with Larose in the manner suggested by the Examiner.

Fourth---and by itself enough to distinguish Claim 28 from these references---the Applicant has amended Claim 28 by adding a limitation of *storing*; to clearly show that the *generating* and *sending* of the first set of parameters is done *in response to the executing*, and the *generating* and *sending* of the second set are done *in response to the user instructing* a software application to download the software product.

Aziz does not disclose or suggest Claim 30 dependent on Claim 28

On page 10 paragraph 31 of the last Office Action, the Examiner rejects Claim 30 under 35 U.S.C. 103(a) cited Larose further in view of U.S. pat. No. 5, 604, 803 (Aziz). The Applicant respectfully disagrees.

At the Aziz passage cited by the Examiner; Aziz discloses the assignment of passwords to a client workstation where the

“password is valid only for a pre-determined time period (t), such that any delay beyond the time period (t) in accomplishing the login by the client workstation results in a timeout, and invalidation of the ...password” (Aziz 2:64-3:1, emphasis added).

If such a timeout has occurred, the client workstation’s password is then deemed invalid, and Aziz teaches that the user must then get a new password: “*In the event of a timeout, the user must obtain a new...password...*” (Aziz 3:1)

These teachings of Aziz are not relevant or related in any way to the limitations of present Claim 30. Aziz's "timeout" has nothing to do with download terminations--for example a TCP/IP "timeout" that causes a download to fail. Also, Aziz's "timeout" does not relate, in any way, to paused downloads or in fact to *downloading* in general. Indeed there is no discussion of 'downloading' within Aziz; and in fact, the word "download" does not exist within the Aziz's Patent. In short, there is no relationship between Aziz's "timeout" and a paused or failed download. Therefore, if one skilled in the art where to apply the teachings of Aziz in an attempt to perform Claim 30, when a download fails or is paused, and the if Aziz's timeout period has not elapsed, the download would resume without re-authentication of the user's computer---in direct contradiction to Claim 30.

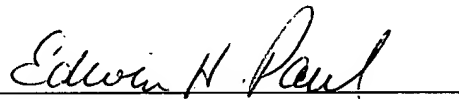
On page 1, item 33, of the Office Action claim 20 and 26 were found allowable if limitations of base claims were included. Applicant agrees with the Office Action, but further as now amended all remaining claims are allowable.

No new matter is introduced by the present amendment.

Therefore it is respectfully requested that a notice of allowance be issued for the present invention as now claimed.

Please charge any additional fee occasioned by this paper to our Deposit Account No. 03-1237.

Respectfully submitted,



Edwin H. Paul
Reg. No. 31,405
CESARI AND MCKENNA, LLP
88 Black Falcon Avenue
Boston, MA 02210-2414
(617) 951-2500

IN THE DRAWINGS:

Replacement Formal Drawings are attached hereto.